Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	"20030163683"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 11:12
S2	4	"6584071".pn. "6684336".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/18 14:24
S3	523	713/153.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/18 15:17
S4	99	("6128279" "6262984" "6310877" "5903559" "6147971" "6594235" "6728779" "6567380" "5802313" "6173364" "6178172" "5722418" "5924094" "6002930" "6208623" "6212188" "6212188" "6363065" "6446092" "6463061" "6463471" "6532237" "6614757" "6914886" "6396842" "6456600" "6473408" "5687319" "6470022" "6483808" "6577653" "6760777" "5642350" "5968133" "6061734" "6061734" "6112245" "6202094" "6392997" "6512768" "6614809" "6643279" "6839771" "6853617" "6865599" "6941355" "6065062" "6112249" "5504757" "5867648").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/18 16:09
S5	23	((secure private anonymous secret concealed) with path) SAME multi$1cast	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/18 16:13
S6	2	(LSP label$1switched$1path) AND (encrypt$3 same (label index) same path)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 11:31
S7	37	(LSP label$1switched$1path) with (priva$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 13:49
S8	13	("4870639" | "5233604" | "5999286" | "6301244" | "6321271" | "6347078" | "6377551").PN. OR ("6584071").URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2005/10/19 12:02

S9	1	S8 and (privacy)	US-PGPUB; USPAT; USOCR	OR	OFF	2005/10/19 12:03
S10	4	(FEC forwarding$1equivalent$1class) with privacy	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 14:10
S11	7	encrypt$3 with path with index	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 14:21
S12	6	encrypt$3 with path with label	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 14:27
S13	1	anonym$5 same path same peer same label	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 14:28
S14	2	anonym$5 and encrypt$3 and (path same peer same label)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 15:45
S15	2	(anonym$5 same peer) and encrypt$3 and (path same label)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 14:30
S16	245	anonym$5 and peer and encrypt$3 and path and label	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 14:30
S17	171	S16 and @ad<"20020228"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 14:31
S18	2	(p2p peer$1to$1peer peer$12$1peer) SAME anonym$5 SAME path	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 16:06

S19	24	(p2p peer$1to$1peer peer$12$1peer) AND anonym$5 SAME path	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 16:07
S20	63	(p2p peer$1to$1peer peer$12$1peer) SAME anonym$5 AND path	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/19 16:07
S21	6	("5862223" "6460036").pn. "20020128871"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/10/20 14:05

Freenet: A Distributed Anonymous Information Storage and Retrieval System (2000) (Make Corrections) (368 citations)

Ian Clarke, Oskar Sandberg, Brandon Wiley, Theodore W. Hong
Lecture Notes in Computer Science

Abstract: We describe Freenet, an adaptive peer-to-peer network application that permits the publication, replication, and retrieval of data while protecting the anonymity of both authors and readers. Freenet operates as a network of identical nodes that collectively pool their storage space to store data files and cooperate to route requests to the most likely physical location of data. No broadcast search or centralized location index is employed. Files are referred to in a location-independent... (Update)

Cited by: **More**
Software Environment of a Grid-based Virtual - Organization For Flood (2004) (Correct)
The LOCKSS Peer-to-Peer Digital - Preservation System Petros (2005) (Correct)
Indexing Distributed Complex Data for Complex Queries - Egemen Tanin Department (2004) (Correct)

Similar documents (at the sentence level):
46.8%: Design Issues in - Anonymity And Unobservability (2000) (Correct)
46.3%: Freenet: A Distributed Anonymous Information Storage.. - Clarke, Sandberg.. (2000) (Correct)

Active bibliography (related documents): **More** **All**
0.5: Information Hiding, Anonymity and Privacy: A Modular Approach - Hughes, Shmatikov (2002) (Correct)
0.2: Protecting Free Expression Online with Freenet - Clarke, Miller, Hong.. (2002) (Correct)
0.2: The Persistence of Memory in Freenet - Hong, Clarke (Correct)

Similar documents based on text: **More** **All**
0.2: Community, Joining, and Specialization in Open Source.. - von Krogh, Spaeth.. (2003) (Correct)
0.1: Using the Small-World Model to Improve Freenet Performance - Zhang, Goel, Govindan (2002) (Correct)
0.1: FASD: A Fault-tolerant, Adaptive, Scalable, Distributed Search.. - Kronfol (2002) (Correct)

Related documents from co-citation: **More** **All**
45: Chord: A scalable peer-to-peer lookup service for Internet applications - Stoica, Morris et al. - 2001
44: A scalable content-addressable network - Ratnasamy, Francis et al. - 2001
28: OceanStore: An Architecture for Global-Scale Persistent Storage - Kubiatowicz - 2000

BibTeX entry: **(Update)**

Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. Freenet: A Distributed Anonymous Information Storage and Retrieval System. In Proc. of the ICSI Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, 2000. International Computer Science Institute. http://citeseer.ist.psu.edu/clarke00freenet.html More

```
@article{ clarke01freenet,
    author = "Ian Clarke and Oskar Sandberg and Brandon Wiley and Theodore W. Hong",
    title = "Freenet: {A} Distributed Anonymous Information Storage and Retrieval System",
    journal = "Lecture Notes in Computer Science",
    volume = "2009",
    pages = "46--??",
    year = "2001",
    url = "citeseer.ist.psu.edu/clarke00freenet.html" }
```

Citations (may not include all citations):
159 Private information retrieval - Chor, Goldreich et al. - 1998 ACM DBLP
149 Collective dynamics of 'small-world' networks (context) - Watts, Strogatz - 1998
104 The Eternity service - Anderson - 1996
101 The Free Haven project: distributed anonymous storage servic.. - Dingledine, Freedman et al. - 2001 DBLP
92 The small world problem (context) - Milgram - 1967
75 Untraceable electronic mail, return addresses, and digital p.. (context) - Chaum - 1981 ACM DBLP
70 A prototype implementation of archival intermemory - Chen, Edler et al. - 1999 ACM DBLP
57 Onion routing for anonymous and private Internet connections - Goldschlag, Reed et al. - 1999
53 Error and attack tolerance of complex networks (context) - Albert, Jeong et al. - 2000

34 Web MIXes: a system for anonymous and unobservable Internet .. - Berthold, Federrath et al. - 2001 DBLP
28 A distributed decentralised information storage and retrieva.. - Clarke - 2000
26 TAZ servers and the rewebber network: enabling anonymous pub.. - Goldberg, Wagner - 1998 DBLP
23 Anonymous web transactions with Crowds - Reiter, Rubin - 1999 ACM DBLP
22 Public Key Cryptography for the Financial Services Industry .. (context) - Standards, American - 1997
20 Growth dynamics of the world-wide web (context) - Huberman, Adamic - 1999
15 Publius: a robust, tamper-evident, censorship-resistant, web.. - Waldman, Rubin et al. - 2000
4 Performance (context) - Hong - 2001 ACM
3 Church of Spiritual Technology (context) - Spiritual, Dataweb et al. - 1999
3 Prentice-Hall: Upper Saddle River (context) - Tanenbaum, Systems - 1992
2 The INDIA protocol (context) - Ellard, Megquier et al. - 2000
2 Several web sites are attacked on day after assault shut Yah.. (context) - Richtel, Robinson - 2000
2 Frequently asked questions about Mixmaster remailers (context) - Cottrell - 2000
2 The eroded self (context) - Rosen - 2000
1 The Slashdot e#ect: an analysis of three Internet publicatio.. (context) - Adler - 1999

Year of Publication of Citing Articles
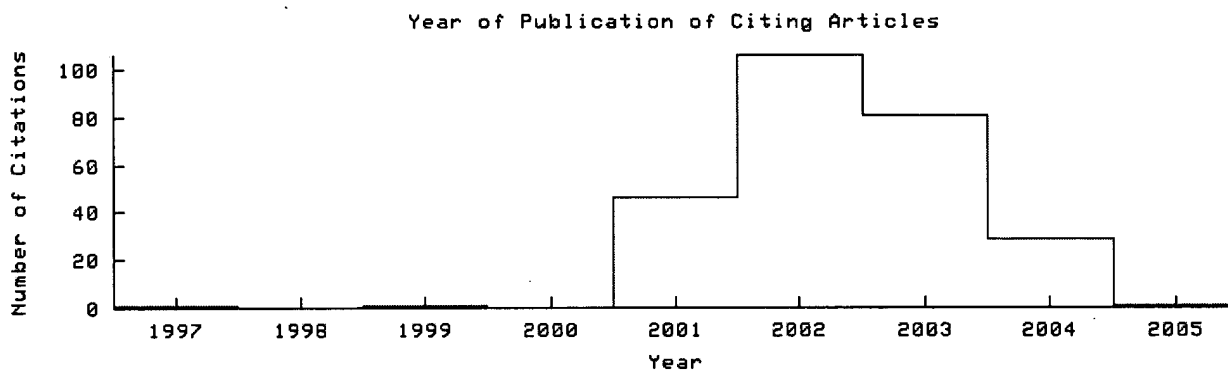
The graph only includes citing articles where the year of publication is known.

Documents on the same site (http://www.pdos.lcs.mit.edu/6.824/papers/): More
Providing Persistent Objects in Distributed Systems - Liskov, Castro, Shrira, Adya (1999) (Correct)
Scheduler Activations: Effective Kernel Support for.. - Anderson, Bershad.. (1992) (Correct)
Design and Implementation of the Sun Network Filesystem - al. (1985) (Correct)

Online articles have much greater impact   More about CiteSeer.IST   Add search form to your site   Submit documents   Feedback

IEEE Xplore®
RELEASE 2.1

Welcome United States Patent and Trademark Office

☐ **Search Session History**

BROWSE   SEARCH   IEEE XPLORE GUIDE   SUPPOF

Edit an existing query or compose a new query in the Search Query Display.

Select a search number (#) to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Wed, 19 Oct 2005, 6:59:35 PM EST

Search Query Display

Recent Search Queries

#1   ((anonymous connections and onion routing)<in>metadata)

#2   ((anonymous connections and onion routing)<in>metadata)

#3   ((anonymous connections and onion routing)<in>metadata)

#4   ((anonymous connections and onion routing)<in>metadata)

Help   Contact Us   Privacy & Security

Indexed by
Inspec

THE ACM DIGITAL LIBRARY

◖ Feedback Report a problem Satisfaction survey

Terms used **Onion routing**   Found **14,030** of **164,603**

Sort results by | relevance ▢ | ❧ Save results to a Binder   Try an Advanced Search
Display results | expanded form ▢ | ❓ Search Tips   Try this search in The ACM Guide
                                          ☐ Open results in a new window

Results 1 - 20 of 200   Result page: **1** 2 3 4 5 6 7 8 9 10   next
Best 200 shown   Relevance scale ☐ ▱ ▭ ▬ ▬

1 Onion routing
David Goldschlag, Michael Reed, Paul Syverson
February 1999 **Communications of the ACM**, Volume 42 Issue 2
Publisher: ACM Press

4 The predecessor attack: An analysis of a threat to anonymous communications systems

Matthew K. Wright, Micah Adler, Brian Neil Levine, Clay Shields

November 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 4

Publisher: ACM Press

Full text available: pdf(295.25 KB)   Additional Information: full citation, abstract, references, index terms

There have been a number of protocols proposed for anonymous network communication. In this paper, we investigate attacks by corrupt group members that degrade the anonymity of each protocol over time. We prove that when a particular initiator continues communication with a particular responder across path reformations, existing protocols are subject to the attack. We use this result to place an upper bound on how long existing protocols, including Crowds, Onion Routing, Hordes, Web Mixes, and D ...

Keywords: Privacy, anonymity, anonymous communication, predecessor attack

5 A protocol for anonymous communication over the Internet

Clay Shields, Brian Neil Levine

November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(720.32 KB)   Additional Information: full citation, references, citings, index terms

6 Networking: Trust based adaptive on demand ad hoc routing protocol

Rajiv K. Nekkanti, Chung-wei Lee

April 2004 **Proceedings of the 42nd annual Southeast regional conference**

Publisher: ACM Press

Full text available: pdf(283.49 KB)   Additional Information: full citation, abstract, references

In this paper, we propose a routing protocol that is based on securing the routing information from unauthorized users. Even though routing protocols of this category are already proposed, they are not efficient, in the sense that, they use the same kind of encryption algorithms (mostly high level) for every bit of routing information they pass from one intermediate node to another in the routing path. This consumes lot of energy/power as well as time. Our routing algorithm basically behaves dep ...

Keywords: AODV, ad-hoc routing protocol, encryption/decryption, security level, trust factor

7 Sensor networks: Source-location privacy in energy-constrained sensor network routing

Celal Ozturk, Yanyong Zhang, Wade Trappe

October 2004 **Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks**

Publisher: ACM Press

Full text available: pdf(209.79 KB)   Additional Information: full citation, abstract, references, index terms

As sensor-driven applications become increasingly integrated into our lives, issues related to sensor privacy will become increasingly important. Although many privacy-related issues can be addressed by security mechanisms, one sensor network privacy issue that cannot be adequately addressed by network security is confidentiality of the source sensor's location. In this paper, we focus on protecting the source's location by introducing suitable modifications to sensor routing protocols to mak ...

Keywords: context privacy, flooding, sensor networks privacy, source-location privacy

8 Peer to peer networks: Tarzan: a peer-to-peer anonymizing network layer

Michael J. Freedman, Robert Morris
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**

Full text available: pdf(242.72 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

Tarzan is a peer-to-peer anonymous IP network overlay. Because it provides IP service, Tarzan is general-purpose and transparent to applications. Organized as a decentralized peer-to-peer overlay, Tarzan is fault-tolerant, highly scalable, and easy to manage.Tarzan achieves its anonymity with layered encryption and multi-hop routing, much like a Chaumian mix. A message initiator chooses a path of peers pseudo-randomly through a restricted topology in a way that adversaries cannot easily influenc ...

Keywords: IP tunnels, anonymity, cover traffic, distributed trust, mix-nets, overlay networks, peer-to-peer

9 An on-demand secure routing protocol resilient to byzantine failures

Baruch Awerbuch, David Holmer, Cristina Nita-Rotaru, Herbert Rubens
September 2002 **Proceedings of the 3rd ACM workshop on Wireless security WiSE '02**

Full text available: pdf(233.97 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>citings</u>, <u>index terms</u>

An ad hoc wireless network is an autonomous self-organizing system ofmobile nodes connected by wireless links where nodes not in directrange can communicate via intermediate nodes. A common technique usedin routing protocols for ad hoc wireless networks is to establish therouting paths on-demand, as opposed to continually maintaining acomplete routing table. A significant concern in routing is theability to function in the presence of byzantine failures whichinclude nodes that drop, modify, or m ...

Keywords: ad hoc wireless networks, byzantine failures, on-demand routing, security

10 Secure traceroute to detect faulty or malicious routing

Venkata N. Padmanabhan, Daniel R. Simon
January 2003 **ACM SIGCOMM Computer Communication Review**, Volume 33 Issue 1

Full text available: pdf(233.68 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

Network routing is vulnerable to disruptions caused by malfunctioning or malicious routers that draw traffic towards themselves but fail to correctly forward the traffic. The existing approach to addressing this problem is to secure the routing protocol by having it validate routing updates, i.e., verify their authenticity, accuracy, and/or consistency. In this paper, we argue that it is also important to ensure the robustness of packet forwarding itself. To this end, we propose a different appr ...

11 Flocks: distributed proxies for browsing privacy

Martin S. Olivier
October 2004 **Proceedings of the 2004 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries SAICSIT '04**

Full text available: pdf(110.65 KB)   Additional Information: <u>full citation</u>, <u>abstract</u>, <u>references</u>, <u>index terms</u>

This paper introduces a Privacy-Enhancing Technology (PET) based on a hybrid of Crowds and anonymising proxies. The PET--referred to as Flocks --operates by establishing a number of Web proxies and letting these proxies randomly forward requests to other proxies (or the final destination). This distributes users' requests over a number of such proxies, thereby helping to protect their (browsing) privacy.

The problem that the paper considers is the effect of two primary design parameter ...

12 Personal trusted devices for web services: revisiting multilevel security

Edgar Weippl, Wolfgang Essmayr

April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

Full text available: ⬛ pdf(109.95 KB)   Additional Information: full citation, abstract, references, index terms

In this paper we revisit the concept of mandatory access control and investigate its potential with personal digital assistants (PDA). Only if applications are clearly separated and Trojans cannot leak personal information can these PDAs become personal trusted devices. Limited processing power and memory can be overcome by using Web services instead of full-fledged applications - a trend also in non-mobile computing. Web services, however, introduce additional security risks, some of them speci ...

Keywords: multilevel security (MLS), personal digital assistant (PDA), personal trusted device (PTD), trusted computing base (TCB)

13 Communication privacy: Location diversity in anonymity networks

Nick Feamster, Roger Dingledine

October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society**

Publisher: ACM Press

Full text available: ⬛ pdf(181.61 KB)   Additional Information: full citation, abstract, references, index terms

Anonymity networks have long relied on diversity of node location for protection against attacks---typically an adversary who can observe a larger fraction of the network can launch a more effective attack. We investigate the diversity of two deployed anonymity networks, Mixmaster and Tor, with respect to an adversary who controls a single Internet administrative domain.

Specifically, we implement a variant of a recently proposed technique that passively estimates the set of administra ...

Keywords: anonymity, interdomain routing, mix networks

14 A survey of peer-to-peer content distribution technologies

Stephanos Androutsellis-Theotokis, Diomidis Spinellis

December 2004 **ACM Computing Surveys (CSUR)**, Volume 36 Issue 4

Publisher: ACM Press

Full text available: ⬛ pdf(517.77 KB)   Additional Information: full citation, abstract, references, index terms

Distributed computer architectures labeled "peer-to-peer" are designed for the sharing of computer resources (content, storage, CPU cycles) by direct exchange, rather than requiring the intermediation or support of a centralized server or authority. Peer-to-peer architectures are characterized by their ability to adapt to failures and accommodate transient populations of nodes while maintaining acceptable connectivity and performance.Content distribution is an important peer-to-peer application ...

Keywords: Content distribution, DHT, DOLR, grid computing, p2p, peer-to-peer

15 Privacy through pseudonymity in user-adaptive systems

Alfred Kobsa, Jörg Schreck

May 2003 **ACM Transactions on Internet Technology (TOIT)**, Volume 3 Issue 2

Publisher: ACM Press

Full text available: ⬛ pdf(881.69 KB)   Additional Information: full citation, abstract, references, citings, index terms, review

User-adaptive applications cater to the needs of each individual computer user, taking for

example users' interests, level of expertise, preferences, perceptual and motoric abilities, and the usage environment into account. Central user modeling servers collect and process the information about users that different user-adaptive systems require to personalize their user interaction.Adaptive systems are generally better able to cater to users the more data their user modeling systems collect and ...

Keywords: Chaum mix, KQML, User modeling, access control, anonymity, encryption, personal information, personalization, privacy, pseudonymity, reference model, secrecy, security, user-adaptive systems

16 Digital village: Anonymizing the net

Hal Berghel, Kim Womack
April 2003 **Communications of the ACM**, Volume 46 Issue 4
Publisher: ACM Press
Full text available: pdf(130.14 KB)
html(24.78 KB) Additional Information: full citation, abstract, index terms

Sanitizing packets for fun and profit.

17 SOS: secure overlay services

Angelos D. Keromytis, Vishal Misra, Dan Rubenstein
August 2002 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications**, Volume 32 Issue 4
Publisher: ACM Press , ACM Press

Full text available: pdf(210.90 KB) Additional Information: full citation, abstract, references, citings, index terms

Denial of service (DoS) attacks continue to threaten the reliability of networking systems. Previous approaches for protecting networks from DoS attacks are reactive in that they wait for an attack to be launched before taking appropriate measures to protect the network. This leaves the door open for other attacks that use more sophisticated methods to mask their traffic.We propose an architecture called Secure Overlay Services (SOS) that proactively prevents DoS attacks, geared toward supportin ...

Keywords: denial of service attacks, network security, overlay networks

18 Communication privacy: Minx: a simple and efficient anonymous packet format

George Danezis, Ben Laurie
October 2004 **Proceedings of the 2004 ACM workshop on Privacy in the electronic society**
Publisher: ACM Press
Full text available: pdf(154.03 KB) Additional Information: full citation, abstract, references, index terms

<i>Minx</i> is a cryptographic message format for encoding anonymous messages, relayed through a network of Chaumian mixes. It provides security against a passive adversary by completely hiding correspondences between input and output messages. Possibly corrupt mixes on the message path gain no information about the route length or the position of the mix on the route. Most importantly Minx resists active attackers that are prepared to modify messages in order to embed tags which they ...

Keywords: anonymity, mix networks, tagging attacks

19 Normalizing Traffic Pattern with Anonymity for Mission Critical Applications

Dongxi Liu, Chi-Hung Chi, Ming Li
April 2004 **Proceedings of the 37th annual symposium on Simulation**
Publisher: IEEE Computer Society
Full text available: pdf(136.16 KB) Additional Information: full citation, abstract

Intruders often want to analyze traffic pattern to getinformation for his some malicious activities inultra-secure network. This paper presents a generalapproach to prevent traffic

pattern of IP-based networkfrom being analyzed. It is an isolated scheme which canbe used to prevent traffic analysis in overall network byachieving the same goal in each network segmentindependently. On each network segment,complementary traffic is generated according to its realtraffic, and the combination of these ...

20 The architecture of robust publishing systems

Marc Waldman, Aviel D. Rubin, Lorrie Faith Cranor
Full text available: pdf(680.21 KB)   Additional Information: full citation, abstract, references, index terms

The Internet in its present form does not protect content from censorship. It is straightforward to trace any document back to a specific Web server, and usually directly to an individual. As we discuss below, there are valid reasons for publishing a document in a censorship-resistant manner. Unfortunately, few tools exist that facilitate this form of publishing. We describe the architecture of robust systems for publishing content on the Web. The discussion is in the context of Publius, as that ...

Keywords: Censorship resistance, Web publishing

Useful downloads: Adobe Acrobat   QuickTime   Windows Media Player   Real Player